DENTONS

DENTONS GOVERNMENT CONTRACTS ACADEMY
VIRTUAL | 2021

CYBERSECURITY PANEL DISCUSSION

Presenters:

Elisabeth Pinsonneault, United Launch Alliance LLC Attorney

Sylvia Gaffney, Viasat Inc. Associate General Counsel

Jeffrey Bauer, Viasat Inc. Government Products & Services Segment Lead for Cybersecurity, Risk Management & Compliance

Phillip Seckman, Dentons Partner

March 11, 2020

Welcome

Welcome to our Dentons Academy webinar series

We are excited to continue to bring our clients practical analysis of recent decisions, statutes, regulations, trends and other hot topics impacting the government contracting community.

Join us for the next Dentons Academy webinar

Ethics in government contracting

Understanding the ethical and compliance rules that apply to the federal government marketplace - Thursday, May 6, 2021, 12-1 pm ET

Agenda

- Overview of the Cybersecurity Regulations
- Defense Contract Management Agency (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) Reviews
- Cybersecurity Maturity Model Certification (CMMC) Planning and Requirements
- Developments based on Cybersecurity In the News
- Question & Answer

Overview of the Cybersecurity Regulations

Background

- E.O. 13556 (Nov. 4, 2010) - Designated NARA as the Executive Agent for the CUI Program
  - 2016 - NARA Issues Final Regulations establishing the required controls and markings for CUI government wide (32 C.F.R. Part 2002)
  - NARA engaged with National Institute of Standards and Technology ("NIST") and DOD to define security controls for non-federal systems and organizations
    - NIST is a non-regulatory agency of the Dept. of Commerce

- NIST SP 800-171 (2015), rev. 2 (Jan. 28, 2021)
  - Purpose: to recommend security requirements for protecting the confidentiality of CUI resident on a nonfederal system
  - May apply to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components

Requirements – 14 “Families”

Requirement “Families”: NIST SP 800-171, rev 2 - Chapter 3	
3.1 - Access Control	3.8 - Media Protection
3.2 - Awareness & Training	3.9 - Personnel Security
3.3 - Audit & Accountability	3.10 - Physical Protection
3.4 - Configuration Management	3.11 - Risk Assessment
3.5 - Identification & Authentication	3.12 - Security Assessment
3.6 - Incident Response	3.13 - System & Communications Protection
3.7 - Maintenance	3.14 - System & Information Integrity

- Each “family” has specific security requirements (basic and derived)
  - More than 100 total requirements, comprised of a blend of policy/procedure- and operational-type requirements
  - Include (among other things) controls for user authentication, user access, media protection, incident response, vulnerability management, and confidentiality of information
- System Security Plans (“SSPs”) and Plans of Action and Milestones (“POAMs”)
- NIST SP 800-171A - “Assessing Security Requirements for Controlled Unclassified Information”
- NIST MEP Self-Assessment Handbook

Compliance Mandated by DFARS

- DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting
  - Contractors must "provide adequate security on all covered contractor information systems"
  - Express incorporation of NIST 800-171 requirements, current on award
  - Cyber incident reporting
    - "Rapidly report" (i.e., within **72 hours** of discovery of any cyber incident via http://dibnet.dod.mil)
    - Review for evidence of compromised covered defense information
    - Media preservation (i.e., preserve and protect images of affected systems for 90 days)
    - DoD access to information / equipment for forensic analysis
  - Malicious software (isolate and submit to DoD Cyber Crime Center (DC3))
- For those with the clause, compliance was required as soon as practicable, but no later than December 31, 2017
- DoD Instruction 5200.48 - established DOD CUI policy (March 6, 2020)

DFARS 252.204-7008

- Solicitation Provision, with the same broad applicability as the CDI clause
  - Calls on contractors to “represent” that, by submission of their offer, the contractor “will implement” NIST SP 800-171 not later than December 31, 2017
  - Alternatively, if the offeror proposes to vary from any of the security requirements of NIST SP 800-171, must submit a written explanation for consideration

FAR 52.204-21 - Basic Safeguarding Rule

- Covers Federal Contract Information
- Less onerous than the NIST SP 800-171 controls
  - No multi-factor authentication
  - No training obligations
  - No system control description requirements
- No reporting requirement for cyber incidents
  - A cyber breach is not considered a breach of the contract "as long as the safeguards are in place”
- Expected to be removed when the NARA FAR Rule is promulgated

DIBCAC Reviews

Developments Leading to DIBCAC Reviews

- **Fahey Memo (December 2018)**
  - Provided contractual language for the government to include in SOW / CDRL allowing access to/requiring delivery of:
    - The contractor's SSP, and
    - The contractor's plan to track flow down of covered defense information and assess compliance of Tier 1 suppliers
- **Lord Memo (January 2019)**
  - Tasked DCMA with "validat[ing]" contractors' NIST compliance via CPSR
  - Focused on flow down to Tier 1 suppliers only
- **Lord Memo (February 2019)**
  - Directed DCMA to identify methods to assess contractor SSPs, and any associated plans of action, "strategically (not contract-by-contract)"
- **DoD IG Audit & Report (July 23, 2019)**
  - Non-statistical sample of 26 (of 12,075) contractors. DoD audited 9.
  - Recommendation included assessing contractor compliance as part of source selection criteria

DCMA Defense Industrial Base Cybersecurity Assessment Center (DIBCAC)

- Interim Rule effective November 30, 2020 adds:
  - DFARS § 252.204–7019, Notice of NIST SP 800–171 DoD Assessment Requirements - Solicitation Provision
  - DFARS § 252.204–7020, NIST SP 800–171 DoD Assessment Requirements - Contract Clause
- Levels of assessments:
  - Basic (Contractor Self-Assessment)
  - Medium (Basic + DoD review, followed by thorough document review and discussion with contractor to obtain additional information or clarification)
  - High (Medium + DoD Onsite Verification)
- Assessment includes Scoring Template that identifies that, while NIST does not prioritize requirements in terms of impact, certain requirements have more impact than others

DIBCAC Assessments

- DIBCAC has provided to contractors a list of items that should be available to the assessment team upon arrival for High Level Assessments:
  - Network Topology Diagram / Network Enterprise Overview Briefing for the Enterprise Unclassified System that has CUI traversing it
  - System security plan(s) and any associated plans of action
  - Demonstration of how the organization manages contractual (lower level) system security plans
  - Results of a Basic Assessment, to include the total score for each system / system security plan assessed (e.g., 105 out of 110) and the date that a score of 110 is expected to be achieved for each system security plan assessed (i.e., all requirements implemented)
  - Subject Matter Experts to be available for the interviews for each control
- DIBCAC identifies that prime contractors could use assessment criteria to evaluate subcontractors

Cybersecurity Maturity Model Certification (CMMC)

CMMC – Purpose

- Interim Rule adds DFARS § 252.204-7021, Cybersecurity Maturity Model Certification Requirements
  - Effective September 30, 2025 (phased roll out prior to then, with requirement to obtain approval from the Under Secretary of Defense for inclusion in a solicitation prior to September 30, 2025).
- What is CMMC?
  - A certification verifying that a contractor can adequately protect sensitive unclassified information such as FCI and CUI at a given certification level, accounting for information flowed down to its subcontractors in a multi-tier supply chain.
  - Based on multiple cybersecurity standards, frameworks, and other references, as well as inputs from industry.

CMMC – Framework & Implementation

- Five Levels of Contractor Certification
  - Risk based approach informs the levels, reflecting a spectrum (e.g., “Basic Cybersecurity Hygiene” to “Advanced”)
  - Companies that process, store, or transmit CUI must achieve at least a CMMC Level 3 certification.

Level	Description
1	15 basic safeguarding requirements from FAR clause 52.204–21
2	65 security requirements from NIST SP 800–171 implemented via DFARS clause 252.204–7012, 7 CMMC practices, and 2 CMMC processes
3	All 110 security requirements from NIST SP 800–171, 20 CMMC practices (i.e., 13 beyond Level 2), and 3 CMMC processes
4	All 110 security requirements from NIST SP 800–171, 46 CMMC practices (i.e., 26 enhanced security requirements above Level 3), and 4 CMMC processes
5	All 110 security requirements from NIST SP 800–171, 61 CMMC practices (i.e., 15 enhanced security requirements above Level 4), and 5 CMMC processes

Developments based on Cybersecurity In the News

DENTONS

Cybersecurity Headlines


DENTONS
DENTONS GOVERNMENT
CONTRACTS ACADEMY
VIRTUAL | 2021
Questions?

Thank you

Dentons US LLP
1400 Wewatta Street
Suite 700
Denver, CO 80202-5548
United States

Dentons is the world's largest law firm, delivering quality and value to clients around the globe. Dentons is a leader on the Acritas Global Elite Brand Index, a BTI Client Service 30 Award winner and recognized by prominent business and legal publications for its innovations in client service, including founding Nextlaw Labs and the Nextlaw Global Referral Network. Dentons' polycentric approach and world-class talent challenge the status quo to advance client interests in the communities in which we live and work. www.dentons.com.